IV.

CRYPTOGRAPHY IN POLITICS.

OLD as the art of cryptography is, it may be doubted whether it has made great advances in modern times. The need of it is not so pressing as it used to be. "How often," says Mr. Philip Thicknesse, an English writer on the art of deciphering, "do we not hear of a courier being murdered and his dispatches carried off, and for what other purpose but information? and, without the key to decipher letters so written, to what purpose should they be intercepted by such a deed?" Mr. Thicknesse wrote only a hundred years ago; but already there has been so great an improvement in the morals of governments that the custom of killing foreign-office messengers for the sake of their dispatch-bags is practically obsolete in diplomacy, and statesmen have ceased to pillage post-offices or rifle portmanteaus. If they wish for secret papers now, they serve a writ. The telegraph, moreover, has made many of the most difficult of the old codes of cipher unavailable. In this category must be placed all those composed of arbitrary marks, or of words or letters arranged in peculiar positions—in squares, parallelograms, columns, etc. Dr. William Blair, the author of an interesting though now antiquated treatise on "Cipher" in Rees's "Cyclopædia," gives many curious specimens of alphabets constructed of arbitrary signs. Charles I. used a code consisting of short strokes in various positions on a line. The Marquis of Worcester invented a cipher composed of dots and lines variously ordered within a geometrical figure. Dr. Blair made one of three dots, placed over, under, or on the line, by which he could represent no fewer than eighty-one letters, figures, or words. Mr. Thicknesse explained with much particularity, and also with a highly successful if not strictly necessary demonstration of the usefulness of secret writing in affairs of state, a plan of conveying information in the disguise of music, the notes, rests, expression-marks, etc., standing for letters.

As cryptography is now used chiefly for telegraphing, modern ciphers must belong to one of three classes: 1. Words or letters having an arbitrary signification. 2. Numbers representing words or letters. 3. Words or letters having their usual signification but standing in a false order.

After all, the art of cryptography loses nothing by being restricted to the ordinary letters and numerals. The ingenuity expended in devising new alphabets of dots, lines, mathematical and astronomical symbols, and fantastic forms was wasted. One code of this kind is as good or as bad as another, all such "plain ciphers," as they are called, in which the meaning of an arbitrary alphabetic sign is invariable, being easily read by the exercise of a little patience. If *a* is always represented in the cipher by the same symbol, it makes no difference to the translator whether that symbol is an arrangement of dots, or the sign +, or the note ♪, or the figure 4, or the letter *x*. The method of solving a common alphabetic cipher depends upon a knowledge of the relative frequency of certain letters and combinations of letters in ordinary writing. Count how many times each cipher is repeated in the dispatch. The commonest is probably *e*, that being the letter most used in our language. Next in order are likely to be *t, a, o, u, i;* afterward *r* and *s;* the rarest letters are *x, q, j, z.* The double letters *ss, tt, ll, dd, mm, nn, oo, ee* are frequent; *ee, ll,* and *ss* are common terminations, so are *s, ed, ty, ly, ing, tion;* *a* and *u* are found as terminals of a very few words—for instance, "sea" and "you"; *on* and *no, to* and [*n*]*ot, of* and *fo* [*r*] often come together in reversed positions; *and* is very common, not only as a word in itself, but as a part of a word; *that, this, there* are also common; the definite and indefinite articles, *the, a, an,* are generally suppressed in telegrams. If the words are properly divided in the cipher the interpretation will be child's play; but in most cases all the words are run together, or else the divisions are purposely misplaced. At the beginning of a word *h, l, m, n, v,* and *y* must always be followed by a vowel; *b* by *l, r,* or a vowel; *q* in any position requires after it a vowel followed by one of the other vowels. Starting with these principles, write opposite the cipher characters all the equivalents which you think you can fix; if you have guessed right, you will soon recognize fragments of words; if you have guessed wrong, some of the letters will be found in impossible combinations, and you must try again. It should be observed that the rule as to the relative frequency of the letters is only a statement of the average computed from a long passage, say of several pages, and it is often at fault in short messages.

A transparent cipher is formed by shifting the alphabet one or more steps forward or back, using *g*, for example, instead of *a*, *h* for *b*, *i* for *c*, and so on. The only tolerably safe alphabetic cipher is one in which the value of every character is constantly changing. A convenient code of this kind is known as the key-word system. It depends upon a table constructed as follows :

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
m	n	o	p	q	r	s	t	n	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

A key-word is chosen, and written over the message which is to be turned into cipher. For example, the message is, "Send me money," and the key-word is "Fox"; the words will then be prepared in this manner :

Foxf ox foxfo
Send me money

Now find the first letter of the key-word (*f*) in the horizontal row at the top of the table, and the first letter of the message (*s*) in the first vertical column at the left. Follow the *s* line till it intersects the *f* column, and take the letter which is found at the point of junction (*x*) as the first letter of the cipher. Get the other letters in the same way. The cipher will read : *xski ab rckjm.* To translate it, the key-word must be written over the cipher—

F o x f   o x   f o x f o
X s k i   a b   r c k j m

and the previous process reversed ; that is to say, find the first letter of the key (*f*) at the top of the table, run down the column until you come to the first letter of the cipher (*x*), and take for the translation the letter which stands in a line with that *x* in the first column at the left of the table, i. e., *s*. This cipher has one weak point : If you guess any word in any part of the message, you can readily discover the key-word from that, and then the whole secret is out. Now, if you know the subject of the correspondence, an inference as to certain words likely to occur in it will not be difficult, and in any case there are some common words which are rarely missing from dispatches of moderate length. Suppose you have the cipher *xski ab rckjm,* and you suspect that it contains the word "money" ; write that word over the first five letters, and see if the table will yield a satisfactory result by the same process last described. It will not. Try the word in connection with other letters ; when it is placed at the end, you solve the enigma, the letters *rckjm* being converted into *foxfo.* This method of interpretation, however, demands so much time and patience, to say nothing of a measure of good luck, that for ordinary purposes the cipher is quite safe. The key-word system is a very old one, but it has recently been improved and published with modifications for military and commercial purposes.

A more convenient and secure cipher was devised by Mr. Robert Slater, Secretary of the French Atlantic Telegraph Company. This is much used by business men, and specimens of it were recently published in the reports of a famous lawsuit. Mr. Slater's code consists of a vocabulary of 25,000 words, numbered consecutively from 1, and any number that may be agreed upon by the confederates is taken as a key. Suppose the message to be, "Send me money," and the key to be 2,500. "Send" in the vocabulary is numbered 20,364 ; add 2,500, and you have 22,864, opposite which stands the word *unbounded.* By the same process of addition, "me" is converted into *pianist*, and "money" into *precipitation*. If the key remains invariable, it may be discovered by the system of trial-guessing already described; but the danger of this could be avoided by changing the key at every step—adding 2,500, for example, to the first number, 2,600 to the second, etc. The system admits of countless variations.

In all important political campaigns the use of a telegraphic cipher seems to be necessary. It would hasten the Reform millennium, however, if such messages—being in no right sense of the word private telegrams, but a part of the apparatus of popular elections—could always be collected by Congress after the close of the contest, and exposed to public view, on the ground that the people ought to know exactly how their business has been conducted. A few of the secret messages of the Republican agents and managers during the exciting days of November and December, 1876, have been examined by various committees of Congress, but they are of little importance, and their simple devices for concealment hardly deserve to be called a cipher. The following is a part of one of Mr. William E. Chandler's dispatches from Florida; the rest of it being in plain English:

> Noyes and Kasson will be here on Monday, and Robinson must go immediately to Philadelphia, and then come here. Can we also have Jones again? Rainy for not more than one tenth of Smith's warm apples. You can imagine what the cold fellows are doing.

Mr. Chandler explained that *Robinson* meant $3,000 to be deposited in Philadelphia. *Jones* was $2,000. *Rainy* indicated favorable prospects. *Smith's warm apples* represented two hundred and fifty majority, and the *cold fellows* were the Democrats. With a few dispatches for comparison, anybody acquainted with the history of the Florida canvass could have read such a cipher.

The search for cipher dispatches on the other side yielded no fewer than thirteen different codes, including in elaborate and ingenious forms and combinations all the classes of ciphers mentioned on a preceding page as being adapted to telegraphic correspondence —letters standing for other letters, and used both with fixed and shifting keys, two letters standing for one, numbers representing letters, numbers representing words and phrases, two numbers representing a single letter, words taken in an arbitrary sense, and words transposed so that the message was unintelligible without a key. In the most important dispatches two or more of these systems were combined to make a cipher within a cipher. A few messages in Oregon were disguised by merely substituting *b* for *a*, and so on through the alphabet; thus, *cfnpsf fyqmjdju* meant "Be more explicit." This solution would occur to almost any intelligent person at first sight; but the cipher was difficult to translate on account of the many blunders which occurred in transmitting it. An alphabet in which every letter was represented by two other letters arbitrarily selected, looked harder. Here is a specimen of it:

Yeeiemnsppaissitpinsititaashshyypiimimnssspeenaaimaennsyisnpinsimimpeaaityyen.

The character of this cipher, however, was easily determined. The abundance of double letters showed that it was not a common alphabetic cipher in which each letter is represented by a single and invariable symbol; and the fact that it contained only ten of the letters of the alphabet proved that it was not read by a shifting key. It must therefore be based upon combinations of letters. This being assumed, a translation was instantly made with the help of a dispatch which was partly in plain English, proper names only being written in cipher. It began: "Gave *ppaishsh* charge of *ityyitns;* he sent to *mapinsimyypiit* but not to the other. Brevard returns sent you to-day." The first cipher word was evidently the name of a person; the second and third appeared to be names of counties. If we suppose each cipher letter to be composed of two characters, we should have for *ityyitns* a word of four letters, the first and third of which are the same. The dispatch belongs to the Florida correspondence, and the only Florida county which meets these conditions is "Dade." The letters of Dade are repeated in the next word, where they fit the interpretation "Brevard"; and all the conjectures so far made accord with the rules respecting the average frequency of letters. Applying the alphabet thus begun to the dispatch quoted above, we obtain the following fragment: " . . *ve* . . . *dred d* . . . *ar.*," which is readily converted into "five hundred dollars"; and the rest follows rapidly.

An alphabetic cipher composed entirely of double numbers gave more trouble. There were not many specimens of it, and it happened that the general rule of the relative frequency of letters was here at fault. The fact that the cipher was double having been determined by the same circumstances observed in the double-letter code, the interpretation was finally obtained by a series of trial-guesses on the following dispatch:

```
8455893193276689272042663455
339320348955553993425533934844
55522766332020553131664227829696
93208266489352279344933482313127
93938248396682203442824893448296
396642488284523166422766755552
4839668233932093395527824866
5248445542824889845596965233
8284664893208233993274893422066
89273193484893429655208268829320662766
7755879382339952338448825533667766
82332748775587934233554284663387662727
82337793319384485542663187554893663320966633
20669652274855966625939684318233663320845534
778233668448829696932082664893318934823131
75932755527744484855965542425534
```

The date, signature, and address led to the supposition that the message might refer to a dispute about the powers of the Governor in canvassing the Presidential returns. The word "canvass" was accordingly searched for, and at the end of the twelfth line the following arrangement of numbers was found: 84, 66, 33, 87, 66, 27, 27. This proved to be a fortunate guess, and, having six letters to begin with, the alphabet was completed without further difficulty.

Three or four codes were studied in which words were used in an arbitrary sense, or numbers substituted for certain "tell-tale" words. These were read, with more or less assurance of correctness, by collating several dispatches and considering the context; but where the number of specimens is small the interpretation of most of the words is no better than guess-work, and it can not be depended upon. These ciphers, however, always excite suspicion, and they were not employed for communications of much importance, except in combination with another system, to be examined later. The "Dictionary Cipher" is a system in which a substitute is found for every word in the message by turning a certain number of pages in a vocabulary previously chosen. The greater part of the Oregon correspondence was conducted in this cipher, the book used being a small "Household English Dictionary," published in London. The secret was betrayed by somebody who had employed the same code in business transactions, and the process of deciphering after that was little more than a mechanical operation. A number of dispatches in a dictionary cipher, however, were found in the Florida and South Carolina bundles, without any clew to the book by which they were made. It was assumed that the volume was a small one, handy to carry in traveling, and that as a matter of convenience the number of pages to be turned would not be more than six or seven. All the small dictionaries accessible were accordingly tried with one of the dispatches, and an easy translation was at last made with "Webster's Pocket Dictionary." The key varied, being applied by turning back sometimes one page, sometimes two, three, four, or five pages. In Oregon the translation went forward instead of back, and the number of pages was always four. The dictionary cipher is clumsy to use, easy to detect, and liable to blunders which are not readily corrected.

By far the largest as well as the most momentous part of the recently disclosed correspondence was conducted by means of an elaborate system of substitution and transposition cipher combined. Arbitrary equivalents were first written in place of the important or "tell-tale" words, and then the whole dispatch was transposed. The substituted equivalents were sometimes proper nouns (generally geographical names, as *America, France, Russia, Copenhagen*), and sometimes numbers. The transposition of the words was made according to fixed rules or sequences of numbers, and the sentences were rearranged for translation by the use of a duplicate key in the hands of the person to whom the dispatch was addressed. Here is a specimen of a message from Columbia to New York ; it is only the beginning of a long telegram, but the sense is complete as far as it goes :

> Now bring safe river thing stuff river Warsaw man would as all Copenhagen to have on Warsaw for Schuylkill through Rochester Schuylkill receiving river the looks at Danube work received.

It is the combination of the transposition and substitution systems which makes this cipher difficult to interpret. Dislocated sentences can be rearranged with a little patience when the meaning of the words is known ; and a substitution cipher, if enough specimens of it are at hand, can be readily interpreted by the context. But here the significance of the most important words and the context are both unknown. The problem, accordingly, is to rearrange a transposed sentence without understanding all the words. The feat would have been almost impossible if the translators had not been supplied with a very large number of dispatches. The first step was a fortunate guess at the meaning of one of the commonest of the substitution ciphers, *Warsaw*. This, after a few trials, was assumed to be "telegram," and the following message of ten words was then easily deciphered :

[Cipher.]

Warsaw they read all unchanged last are idiots cant situation.

[Translation.]

Can't read last telegram. Situation unchanged. They are all idiots.

The same order of words was tried on other telegrams. It would fit messages of just ten words, but no others. Hence the key evidently varied with the length of the dispatch. It was now observed that the number of words in a message was invariably a multiple of five. There were a few telegrams of ten words, a few of fifteen, many of twenty, twenty-five, and so on, and they ran up to two hundred, always proceeding by fives. This showed that the confederates had taken an assortment of sequences, or blocks of numbers, arranged them in some arbitrary order, and adopted them as the keys for transposing and rearranging the dispatches, the number of words in the message being the clew by which the receiver knew what key or combination of keys he must use in the translation. To reconstruct these sequences by collating dispatches of equal length was a work that demanded only time and patience. Five thirty-word telegrams were first written in parallel columns, and every word numbered, thus :

No. of word.	First dispatch.	Second dispatch.	Third dispatch.	Fourth dispatch.	Fifth dispatch.
1..........	Me	Very	Figure	To	Rochester
2..........	you	news	France	situation	of
3..........	do	say	capture	prospects	answer
4..........	to	Copenhagen	and	and	America
5..........	did	to	over	Africa	yesterday
6..........	to	from	what	desperate	to-day
7..........	question	can	see	intend	understands
8..........	when	Florida	answer	Thames	Thomas
9..........	you	you	Europe	soon	my
10	you	count	Moselle	Europe	Africa
11..........	to	much	Russia	report	about
12..........	morning	in	shall	every	but
13..........	asked	be	little	mischief	it
14..........	want	give	and	the	first
15..........	where	what	appearances	Warsaw	avail
16..........	go	Louisiana	about	in	at
17..........	supposed	am	best	dispatch	my
18..........	this	placed	hope	in	nothing
19..........	until	if	Glasgow	acting	Bavaria
20..........	come	mixed	will	this	as
21..........	to-night	insure	up	will	will
22..........	important	London	keep	state	Copenhagen
23..........	and	Oregon	Oregon	all	once
24..........	answer	few	America	concert	fear
25..........	here	intend	be	morning	reported
26..........	Warsawed	things	can	parties	small
27..........	adjourned	out	Potomac	France	by
28..........	to-morrow	a	behind	in	and
29..........	London	us	Edinburgh	and	satisfied
30..........	you.	here.	I.	received.	hope.

The task now was to find an order of the numbers which would make sense in all five columns. To do this, little groups of words were tried together, and tested by comparison with the parallel columns. There were a few phrases which seemed to adjust themselves naturally ; in the first dispatch, for example, we have the words "adjourned until to-morrow," and if we look for a nominative to adjourned we discover that there is no word in the column that will do except *London.* This order of numbers, 29, 27, 19, 28, gives in the second column "us out if a," and the words that precede "us out" are evidently "intend (25) to (5) count" (10). The sequences thus begun are easily continued ; when the path is lost in one column it is found in another ; and so the difficulty about disposing of the "blind words" is avoided.

The proper key for a message of 30 words being ascertained, sequences of 15, 20, and 25 were next constructed in the same manner. Keys of 35 and 40 were also made, but they proved to be merely repetitions of shorter ones, and the work was therefore supposed to be complete with the key of 30. But as the process of translating went on, unexpected difficulties presented themselves. The keys fitted so perfectly in many instances that there could be no doubt of their correctness, but there were some dispatches which they did not fit at all. It was soon discovered that for every one of the five blocks of numbers there were *two* keys, or sequences, either of which the confederates used at pleasure, and still later it appeared that the second set of keys was a mathematical correlative of the first set, so that any dispatch could be translated by either one of two keys. For example, key III. consists of the following sequence of 15 numbers, 8, 4, 1, 7, 13, 5, 2, 6, 11, 14, 9, 3, 15, 12, 10, and the correlative key IV. is 3, 7, 12, 2, 6, 8, 4, 1, 11, 15, 9, 14, 5, 10, 13. The beginning of a certain message is translated according to key III. by numbering the words consecutively from 1 to 15, and then picking them out in the order given above, thus :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Too	last	do	received	answer	night	late	Warsaw	understand	me	don't	want	to	quite	you,	etc.

But precisely the same translation is obtained by writing over the words the figures of the correlative key IV., and then picking out the words in their natural numerical order, thus :

3	7	12	2	6	8	4	1	11
Too	last	do	received	answer	night	late	Warsaw	under-

	15	9	14	5	10	13
stand	me	don't	want	to	quite	you.

The messages having been transposed, the next step was the translation of the substitution ciphers, or "blind words." In most cases this was easily done by the context. Words like *London* (Returning Board), *Rochester* (votes), *Syracuse* (majority), *Ithaca* (Democrats), *Havana* (Republicans), *Copenhagen* (money), were so plain that there could not be a doubt as to their meaning. Others (*Anna*, *Charles*, *Jane*, *Thomas*, *William*, etc.) proved to have no meaning at all; they were "nulls," thrown in to fill out the dispatch to the number of words required for the key, and, when the transposition was effected, they always fell together at the end. Numerals were represented by the names of rivers, and zero by the word *river*. The precise equivalents of several of these ciphers were clearly fixed by the telegrams in which the figures of votes and majorities were reported ; for example, a South Carolina correspondent, after telegraphing the majority for the Hayes electors on the face of the returns, adds, "*Rhine* of Tilden's within *Moselle Thames river* of their lowest." Now, it is known that one of the Democratic electors was only 230 votes behind the lowest Republican elector. That settles the meaning of *Rhine*, *Moselle*, *Thames*, and *river*. The interpretation thus reached is confirmed by numerous other instances. All the other numbers are equally well ascertained; and, in fact, there is hardly a "blind word" in the whole vocabulary—there is certainly none of any importance—of which the meaning is not capable of demonstration.

JOHN R. G. HASSARD.